USAWC STRATEGY RESEARCH PROJECT

ACHIEVING INFORMATION ASSURANCE

by

Lieutenant Colonel Ulmont C. Nanton, Jr.
United States Army

Colonel Thomas J. Williams
Project Advisor

This SSCFP is submitted in partial fulfillment of the requirements imposed on Senior Service College Fellows. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **03 MAY 2004**	2. REPORT TYPE	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Achieving Information Assurance

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Ulmont Nanton

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**49**	

ABSTRACT

AUTHOR: LTC Ulmont C. Nanton, Jr.

TITLE: Achieving Information Assurance

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 49 CLASSIFICATION: Unclassified

Achieving Information Assurance (IA) is an integral factor in the U.S. efforts to strengthen America's homeland security. Technology enhancements have enabled greater efficiency in our business processes. At the same time, we have increased our dependency on technology and thus our vulnerability. While our enemy continues to exploit conventional means to harm us in our homeland, the threat of compromised information systems in critical infrastructure poses an even greater threat to our national security. Technology enables attacks against our way of life from abroad. It is no longer necessary to take the fight to your neighbor. Our inability to secure the very systems that we have become wholly dependent on could very well be the catalyst that exploits our weakness. Information assurance is the application of controls to mitigate the risk of exposure of our information systems. Our current method of dealing with information security is one of reaction. This process is in urgent need of replacement with a system of proactive protection and immediate/automated corrective action. This paper will show that near real time information assurance is achievable.

TABLE OF CONTENTS

PREFACE

Computer viruses are a form of “cyber life” that have had a measurable impact on society. Currently, they pose no insurmountable threat and have become more of a manageable nuisance. There are however, two alarming trends that make these viruses a much greater threat. The rate at which hackers are writing new viruses is high and accelerating at a geometric rate. The change in operations (Network Centric Warfare) facilitated by the monumental leaps in technology, moves this nation toward increasing interconnectivity and interoperability among information systems. The vast number of interconnections made possible by technology has created hidden vulnerabilities. This will enable computer viruses and worms to spread much more rapidly than ever before.

As the military moves toward a greater reliance on networked systems for combat operations, we must consider what steps need to be taken to ensure the availability and reliability of these networks. In a briefing to the National War College on 21 January 2002, Secretary of Defense Donald Rumsfeld stressed that in order for the military to meet two of his six transformation goals of conducting effective information operations and leveraging information technology to give our joint forces a common operational picture; we must “…Protect our information networks from attack... Use information technology to link up different kinds of US forces so that they can in fact fight jointly...”

Our current posture for protecting our information networks from attack employs the use of a layered defense. This defense presents a potentially unique picture to the attacker at each attempt, thus reducing his capability to successfully penetrate our defenses. This method is a best practice based near term solution. It is a reactive approach to an evolutionary challenge. A more deliberate solution would involve preemptive measures, which could also adapt to the changing environment and characteristics of an attack. It could be a model similar to the human body’s autoimmune response. Once a virus is identified as "non-self" the autoimmune system would send agents to destroy the intruder, and remember the characteristics of the attack so that it may store additional antibodies and respond quicker in the future. The most significant benefit of this type of autoimmune response is that it requires no human intervention.

LIST OF ILLUSTRATIONS

LIST OF TABLES

ACHIEVING INFORMATION ASSURANCE

> We know that the threat is real. Where once our opponents relied exclusively on bombs and bullets, hostile powers and terrorists can now turn a laptop computer into a potent weapon capable of doing enormous damage. If we are to continue to enjoy the benefits of the Information Age, preserve our security, and safeguard our economic well-being, we must protect our critical computer-controlled systems from attack
>
> — President Bill Clinton 2000

A TECHNOLOGY POWER

The United States is the world's most technologically advanced power. Along with this dubious distinction, it is also the most exposed nation to the disruption and destruction of its infrastructure by both military and non-military means from anywhere in the world. This nation's critical infrastructure is vital to our economy and national security operations. Although the government is working diligently towards innovative security practices, the private sector manages most of the critical infrastructure. With a primary focus on the bottom line, there is little return on investment (ROI) for security initiatives. Even with policy directives such as The Clinger-Cohen Act of 1996, the private sector has still been very slow at adopting new security practices. The concept of infrastructure protection doesn't present a compelling case to the CEO and the executive board, whose responsibility is to their shareholders and customers. Because the interdependencies of our information systems are based wholly on this critical infrastructure, the government must act in partnership with the private sector in assuring the nations critical infrastructure. This paper will bring awareness to the vulnerability of our interconnected infrastructure, the implications to national security, and our responsibility to put in place mechanisms to defend the Network Infrastructure and proactively seek to eliminate potential hazards to the infrastructure.

The continually changing environment necessitates an evolution from computer security to information assurance. This change in environment is based primarily on the increased interconnectivity of our information systems, the reliance of our critical business processes on these information systems, and our national security have changed the requirement from simple security to assurance of system availability, integrity, and reliability. Computer Security is defined as "measures & controls that ensure the confidentiality, integrity, and availability of information systems (IS) assets,"[1] a concept, which later evolved to information assurance. The requirement to secure information systems is now more than simply ensuring confidentiality, integrity and availability of computers. It is "information operations that protect and defend information and information systems by ensuring their confidentiality, integrity, availability, authentication, and nonrepudiation and recovery of information systems by incorporating protection, detection and reaction capabilities."[2] The solution proposed in this writing to achieve information assurance will include aspects of computer security as part of the formal recommendations. As the nations business processes and defense capabilities move toward e-business and e-government, the need to ensure authentication and non-repudiation of information systems becomes absolute. Information systems are now an integral part of society and the way we do business as opposed to their ad-hoc relevance given in the past. Secretary of Defense Donald Rumsfeld makes it clear that the direction we are headed for our fighting forces will require greater interconnectivity.

> The two truly transforming things, conceivably, might be in information technology and information operation and networking and connecting things in ways that they function totally differently than they had previously. And if that's possible, what I just said, that possibly the single-most transforming thing in our force will not be a weapon system, but a set of interconnections and a substantially enhanced capability because of that awareness.
>
> - Secretary Rumsfeld - Aug 9, 2001

The focus of this paper is to assist senior leaders in discerning those aspects of information security that are relevant toward achieving that enhanced capability. Although the solution to achieving information assurance requires both active and passive defense measures, this paper will focus primarily on the passive measures because the active measures are still evolving and approach classified disclosure. Achieving information assurance is a journey. It is the continual process of assessing risk and applying mitigating control measures. It requires senior leader involvement to prioritize information requirements and security for critical systems and accept the risk associated with less security for non-critical systems. It is unlikely that we will ever see an interconnected computing environment free of vulnerabilities. Even the most secure network is eventually vulnerable without the continual vigilance of vulnerability assessments and risk mitigation activities. Our journey to achieve information assurance is not about achieving a 100% secure system because the system would be unusable and unaffordable. It is about prioritizing what is important and understanding what interdependencies exist between systems.

THE THREAT

Due to the global nature of cyberspace, the vulnerabilities that exist to the global infrastructure upon which this nation and the world depend, are open to the world and exploitable to anyone with desire to do harm or gain strategic advantage over an adversary. These vulnerabilities are potentially the catalyst for the new weapon of the future. The defense and critical infrastructure of this nation are organized and administered through the use of computerized information systems. Thus information assurance is a component of national security. The Defense Information Infrastructure (DII) supports a range of mission functions using Wide Area Networks (WAN) such as the Joint Worldwide Intelligence Communications System (JWICS) and the Secret Internet Protocol Router Network (SIPRNet) for global connectivity. This current information infrastructure, based on dedicated stovepipe networks and custom information systems is the infrastructure of the past. Today, The Department of Defense (DOD) is almost totally dependent on commercial services within the Nationwide Information Infrastructure (NII). Our total dependence on these computerized systems gives rise to new and greater vulnerabilities. As we move to achieve greater systems integration, we must consider these vulnerabilities along with the new technology enabled business processes and operations they enable. We must consider the interconnectivity of these systems as well as their interdependencies. This nation's critical computer infrastructure is the backbone of our economy and national security and its vulnerability is great.

Al Qaeda operatives have clearly indicated a desire to disrupt this nation's and the world economy through either a physical or cyber attack of our critical infrastructure. What we are finding through arrest and interrogation of Al Qaeda operatives are reconnaissance plans of Americas critical computer infrastructure components. Just as we believe the hijackers of 9/11 had training on flight procedures and airport security vulnerabilities, recent Al Qaeda arrest show that Al Qaeda are trained in computer security. As we move toward a more comprehensive program of defending our information systems, we must also consider the legal vulnerability posed by our current laws not keeping pace with the rate of change in technology or the rate of integration of information systems. This leaves this nation and the rest of the world relatively powerless to effectively prosecute cyber crimes in the face of our ever-increasing vulnerability. In addition to our current process for securing our information systems we should also address preemptive measures for defending against cyber attacks. In the current wave of cyber crimes, we tend to catch the amateurs. We are likely missing the professionals.

Several nation states are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power--impacts that, according to the Director of Central Intelligence, can affect the daily lives of Americans across the country.[3] How ready are we to respond to domestic terrorist attacks if the infrastructure is simultaneously attacked? One must question what if terrorist had brought down our communications and emergency response capability during the attacks of 9/11? Not only would such a "blended" attack impede our ability to respond and recover to the physical attack, it would have a detrimental effect on the confidence of the people of this nation in the ability of its government to provide for their security and well being.

To effectively prevent attacks on our information and information systems, we must characterize our adversaries, their potential motivations, and their attack capabilities. Our potential adversaries include:

- Nation States
- Terrorists
- Criminal Elements
- Hackers

Their motivations may be intelligence-gathering, theft of intellectual property, causing embarrassment, or just pride in having exploited a notable target.[4]

The greatest threat to our information systems comes from insiders. The H1B Visa Program may potentially increase this threat. Congress introduced this program to fill the temporary gap created by increased demand and short supply of technologist. The program gives foreigners access to the most advanced components of America's technology industry. *"Tens of thousands of programmers, database specialists, and other technical workers come to the United States each year on "H1B" visas--temporary visas for workers with in-demand technical skills."*[5] An area specifically at risk is software design. This program is producing foreign hi-tech guest workers that would like to remain in a country where their standard of living far exceeds that at home. There are several inquiries into the improper execution of this program due to lax standards for the immigrant workers which could lead to the government sending disenfranchised workers back home at the end of their visas. According to research firm Gartner, Inc., approximately one of 10 U.S. technology jobs will be overseas by the end of 2004**.**[6]

While it is clear that the greatest threat to our information systems and the national infrastructure comes from within by virtue of a disgruntled or disaffected worker who may bypass traditional security measures, the potential for employee abuse under this H1B program is great. Workers may decide to use their skills to create backdoors or other vulnerabilities in the software they are developing to be exploited at a later date. Historically, insiders have been responsible for the vast majority of loss bearing digital security breaches.[7] There are several examples where perpetrators (software developers) have inserted trapdoors in financial software to later steal money undetected. This type of carefully orchestrated and planned attack is becoming more commonplace.[8]

CYBERSECURITY EVENTS

Our nation has two important tasks to accomplish in the event of an attack from cyberspace:

1. Recover from the attack.
2. Prevent what has not yet occurred.

In January 2000 a computer glitch deafened National Security Agency (NSA) satellites for three days, while in July a National Reconnaissance radar-imaging satellite shut down for 12 hours.[9] These events constitute a serious threat to national security. The idea that attacks on information systems to just have fun is no longer an insignificant issue. Attackers have targeted Defense department information systems in the past. The Pentagon now spends annually more than US$1 billion defending its 2.5 million computers against an estimated 80 to 100 daily attacks. The Pentagon's biggest concern is the 'hackability' of its weapons systems. According to a report in Federal Computer Week, a Defense Information Systems agency training CD-ROM discusses an exercise where a US Air Force officer equipped with a laptop hacked into a US Navy ship at sea and fed false navigational data into its computer.[10]

When we consider cyber attacks of today, we find ourselves dealing with an evolution in technology that fuels the spread of viruses. Our requirement for interconnected systems inextricably ties our systems together in a web, which is also responsible for the spread of these viruses. The “SQL Slammer Worm”, the “Sobig.F Worm”, and the “Blaster Worm”, all virus attacks which hit in 2003, were relatively simple attacks. What is changing in these attacks is the method of propagation. As the technology and interconnectivity of our systems evolves, so does the ability for the virus to spread rapidly. The “NIMDA” attack in 2001 doubled its presence every 37 minutes, eventually reaching about 400,000 servers and causing billions in damage. The “SQL Slammer” in 2003 doubled its presence every 8.5 seconds.[11] Catching these attackers has not been difficult due to the unsophisticated nature of their attacks and their inability to cover their tracks. Cyber terrorism on the other hand is likely to pose a totally different picture. The critical infrastructure on which our economy and national security is dependant, is at stake. We as a nation should consider the potential affect of cyber-attacks on the national infrastructure.

To combat this Cyber terrorism, we must focus our attention on what is important. Even though fiscal constraints force us to cut or hold off hiring additional security staff, we should focus our resources on security knowledge and intelligence. We must invest in the development of security knowledge professionals and centralized intelligence gathering to combat this global threat. Terrorist organizations recognize the value of hiring trained professionals and leverage those individuals to meet their goals. Just as the 9/11 attackers were trained in airport security and airport security vulnerabilities, the potential exist that these attackers are currently training in computer security and critical information system vulnerabilities. We should not let this gapping hole in our information system defenses create another catastrophic event such as we experienced on 9/11.

Of the numerous organizational computer security and information assurance programs in the DOD today, many of them do not have rudimentary processes in place to even establish or keep track of all the devices on their networks. This lack of accountability is paramount to information system vulnerability. It is generally the rogue system connected to a DOD network operating undetected which acts as the conduit for a malicious or non-malicious attack. This disparity between information systems accountability for security and information assurance is generally a resourcing or prioritization issue. We must get beyond the simple hurdles of inventory and accountability and begin to map the interdependencies that exist in our information systems. We cannot be prepared to recover from a cyber-attack if we cannot determine the extent of the vulnerabilities that exist due to our dependence on other systems within the infrastructure.

Perhaps a positive factor in our journey to achieve information assurance is the sharing of security problems so that more organizations may understand cyber-attacks. The establishment of a central clearinghouse for reporting cyber attacks happened in November 1988 in response to the needs identified during an Internet security incident. This clearinghouse is more formally known as the Computer Emergency Response Team (CERT). The CERT is a joint venture between the Defense Advanced Research Projects Agency (DARPA) and Carnegie Mellon University’s Software Engineering Institute to develop solutions to known software vulnerabilities and serve as a repository of computer attacks on information systems.

DARPA was given a charter to work with the Internet community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents. The CERT Coordination Center (CERT/CC) resulted from this initiative.[12] The CERT began collecting data in 1988. The diagram bellow shows the number of reported attacks against information systems since 1988. The Director of CERT Coordination Center stated that he estimates that as much as 80 percent of actual security incidents go unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attack or (2) the organization was reluctant to report.[13]

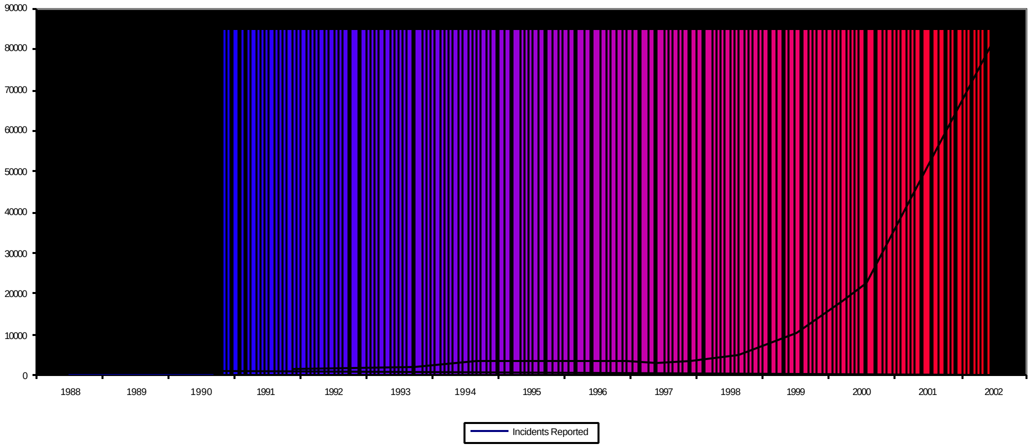

FIGURE 1 CERT STATISTICS ON REPORTED INCIDENTS[14]

While this central clearinghouse may help combat cyber-terrorism, there is resistance from all sectors of government and the private sector about sharing this information. In the private sector, this information could mean the difference between success and failure of the business. The financial sector specifically is the most vulnerable to this concept of information sharing. Other privacy issues such as those posed by the introduction of the Patriot Act have raised concerns about the value warehousing information might have towards discovering terrorist clues.

The Federal Government established several new organizations and policies to assist in combating the threat of cyber-terrorism. Chapter 131 of title 10, United States Code was amended to add Section 2224, Defense Information Assurance Program.[15] We have acquisition reform policies in place to facilitate the development of information systems with security integrated as a part of the system development and life-cycle. Some of this policy guidance is listed below:

- DOD Directive 5000.1, The Defense Acquisition System
- DOD Instruction 5000.2, Operation of the Defense Acquisition System
- DOD Regulation 5000.2-R, Discretionary Guidebook
- Clinger-Cohen Act of 1996
- NSTISSP-11, National IA Acquisition Policy
- DOD Directive 8500.1, Information Assurance
- DOD Instruction 8500.2, Information Assurance Implementation
- DOD IA Strategy
- DOD Instruction 8580.aa, IA Acquisition

In spite of significant initiatives towards reducing our vulnerability, our methods are still primarily reactive. Reacting to these threats will not likely give us any measure of assurance.

> William M. A. Wulf, Ph.D. President, National Academy of Engineering, told the House Science Committee in October 2001 “Based on my experience over the past 30 years, passive defense alone will not work... Effective cyber security must include some kind of active response, some threat; some cost higher than the attacker is willing to pay, to complement passive defense. The practical and legal implications of active defense have not been determined, and the opportunities for mistakes are legion. The international implications are especially troublesome. It is difficult, sometimes impossible, to pinpoint the physical location of an attacker. If the attacker is in another country, could a countermeasure by a U.S. government computer be considered an act of war?”[16]

DEFENSE IN DEPTH

In an effort to achieve a balanced approach to information assurance, the DOD employs a methodology known as Defense in Depth (DID). It is a layered methodology designed to protect the information infrastructure. The DID Strategy is the most effective means to mitigate the risk associated with managing our information systems. It is a strategy based on three principle domains of People, Operations and Technology. It balances the protection, cost, and operational mission needs of an organization. Because all information systems and devices have inherent vulnerabilities, it is best that we defend our resources through a series of defensive layers. DID involves the creation of multiple layers of protection around information systems and critical data. The DOD employs this measure because there are new and innovative types of security threats in today’s environment. The impact of these threats is exacerbated by the use of multiple methods and techniques of propagation. These type threats pose a formidable challenge to legacy security devices because they propagate through existing vulnerabilities in our hardware and software. In DID, a primary goal is to defend against these attacks while simultaneously detecting the attacks. The multiple layers require the attacker to dig deeper to achieve his goal. If we can present a unique picture to the attacker each time he tries to penetrate our defenses while simultaneously increasing his risk of detection, the attack will eventually become unaffordable.

Attacks on information systems are classified as Passive, Active, Outsider, Close-in, and Distributed. Table 1 provides a comprehensive explanation of these attack types.

Attack	Description
Passive	Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capture of authentication information (e.g., pas swords). Passive intercept of network operations can give adversaries indications and warnings of impending actions. Passive attacks can result in disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.
Active	Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These attacks may be mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modific ation of data.
Close-In	Close-in attack consists of a regular type individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry, open access, or both.
Insider	Insider attacks can be malicious or non-malicious. Malicious insiders intentionally eavesdrop, steal or damage information, use information in a fraudulent manner, or deny access to other authorized users. Non-malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as “getting the job done.”
Distribution	Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code into a product, such as a back door to gain unauthorized access to information or a system function at a later date.

TABLE 1 DESCRIPTON OF ATTACK TYPES[17]

Although all attacks should be considered equally important, the insider attack generally presents the greatest threat to information systems and is also virtually undetectable. The reason is simply that insiders have the added advantage of bypassing the typical defenses designed to keep intruders out. They are also knowledgeable in methods of covering their tracks.

Consider the three domains of DID, People, Operations and Technology as representing three concentric rings around the information you are protecting. If you view each ring as rotating in a direction opposite of its proximate ring, then you can see that the sub-domains create a unique picture to an attacker each time they attack. This layered defense allows for protection even if one of the layered defenses fails. See Figure 2 below.

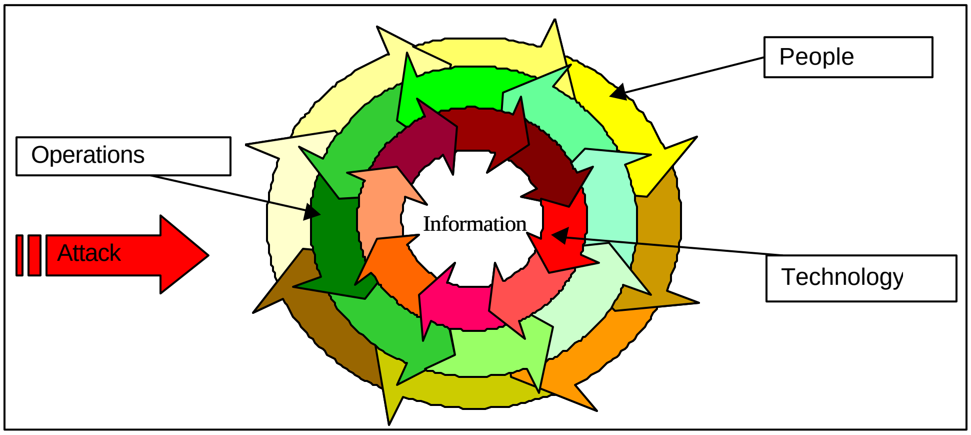

FIGURE 2 DID LAYER METHODOLOGY

PEOPLE

Achieving Information Assurance begins with a senior level management commitment (typically at the Chief Information Officer level) based on a clear understanding of the perceived threat.[18] The People layer is potentially the most important of all layers because it is the first echelon of defense. The majority of attacks on our information systems may be thwarted at this level. Individual users and system administrators are generally a more serious threat than technology because it is harder to detect their malicious activity. Yet we spend most of our resources on defending against technology. This domain of people includes the users of the information systems as well as business partners outside of the enterprise. The categories within the domain people are depicted in Figure 3.

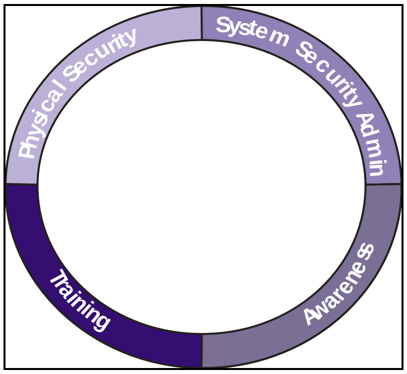

FIGURE 3 DID PEOPLE LAYER

Training

Building, operating, and maintaining secure networks are difficult tasks; and there are few educational and training programs that prepare people to perform them. The increasing need for these skills in organizations has led to assigning information security responsibilities to inexperienced personnel with little or no training or forced organizations to contract the effort.

Training is largely the most overlooked category in the defense of information systems. Attacks are successful against their targets because their targets are unaware of attacker capabilities. Many of today's hacking tools come disguised as a Trojan Horse. Inside these gifts might be hidden code. What minimal training we do accomplish for our users and our Information Technology (IT) staff is primarily how to run and even maintain the system. We seldom apply resources toward the protection of these information systems through training. This critical need for education and increased awareness will help in identifying the characteristics, threats, opportunities, and appropriate behavior in cyberspace.

What we experience today may well be just the tip of the iceberg. Consider how quickly cyberspace developed and how rapidly and effectively it has been exploited for social and economic benefit. Users of these information systems should learn through policy guidance and demonstration when applicable, what is acceptable and unacceptable behavior. In the near term, the greatest need is for short "how to" and "what to be aware of" type training courses. In the long term, the DOD needs to establish a career path for The Information Security Specialist, support undergraduate-level or master's-level specialties in network and information security. Kevin Mitnick is probably the most famous hacker of this century. He penetrated the most sensitive Defense computer systems through social engineering. Even the best security technology investments could not protect information systems from this type of attack. The first line of defense is people with proper training and awareness.

Awareness

Awareness is simply ensuring that all relevant information gets to the lowest level possible. It consists of those events that would inform users and administrators alike of potential threats. Leaders must create a climate of awareness so that users and administrators know what to do when attacks occur. They may accomplish this process through sensible policies, training, and visible action when threats arise.

Physical Security

Physical access is another means for intruders to gain access to our information systems. Physical security is an integral part of information assurance. The physical mechanisms of security must be in place to insure the integrity and confidentiality of our information systems. We must ensure that control mechanisms are in place to prevent unauthorized access to information systems. Leaders must also consider protecting information system assets from environmental hazards.

System Security Administration

Although sometimes perceived as an invasion of privacy, leaders must know and verify the background of employees. There are documented cases where organizations have hired a convicted felon and placed them in charge of sensitive information because they failed to do background checks. Ensure that personnel are trained regularly and are aware of security policies and their individual responsibilities.

TECHNOLOGY

Generally the first solution we reach for is a piece of technology to fix what is broken. While technology is an enabler, it is not the sole answer to our security challenges. To insure that the right technologies are procured and deployed, an organization should establish effective policy and processes for technology acquisition.[19] The components of the Technology domain are depicted at Figure 4.

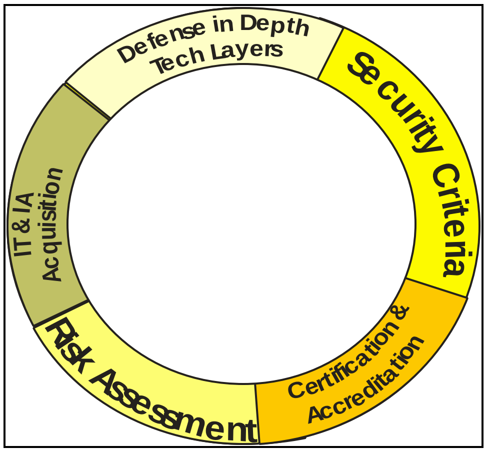

FIGURE 4 DID TECHNOLOGY LAYER

A significant challenge in providing the right technology solution to mitigate infrastructure vulnerabilities and network attacks is the selection of technologies. New and emerging concepts for network defense appear almost daily, all promising the ultimate in protection. Most never make it out of the conceptual stage. The Gartner Group does exhaustive research on these technology devices through what they call a technology “hype cycle”. Gartner defines a hype cycle as “a graphic representation of the maturity, adoption and business application of specific technologies.” [20] Figure 5 shows this cycle with respect to network security devices used for information system and infrastructure protection.

Information security professionals often buy a host of security hardware products, including firewalls, and intrusion-detection systems (IDS), but seldom take the time to understand the functionality those products provide. Perhaps a lack of skills plays a major part in this shortcoming. We must actively manage these devices and review their logs routinely to determine attempts to penetrate the network and successes at penetration.

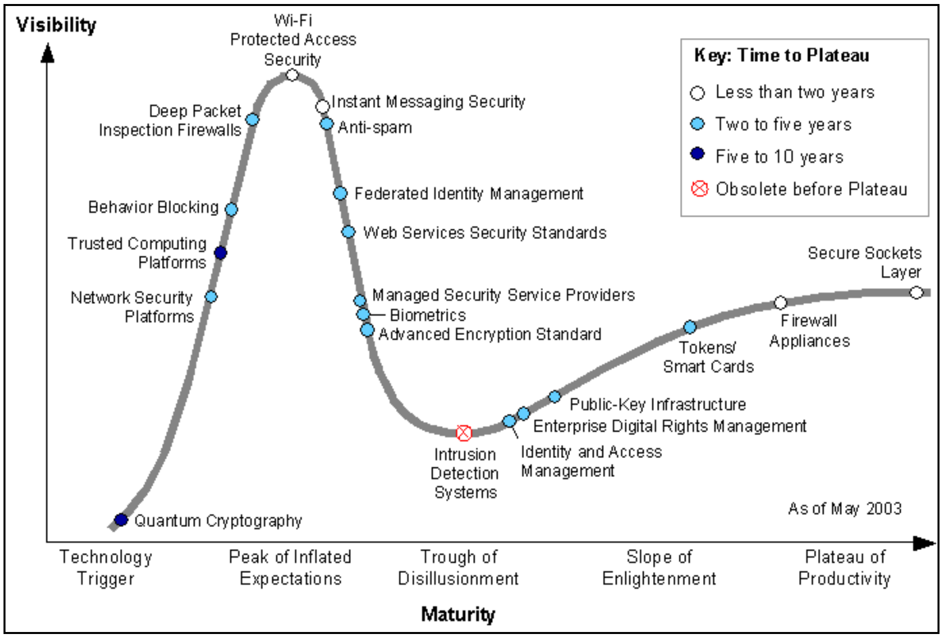

FIGURE 5 GARTNER HYPE CYCLE FOR NETWORK SECURITY DEVICES[21]

Defense In Depth Technical Layers

Defend the computing *environment:* The computing environment is the component of the information architecture that exists at the user level. Defensive actions consist of placing access controls on hosts and servers to resist insider, close-in, and distributed attacks. Other mitigating controls such as anti-virus software, strong authentication and access controls are also considered a part of this layer.

Defend the enclave boundaries: From the user desktop to the first firewall in the systems architecture defines the boundary of the enclave. It is that area of the infrastructure that requires an independent security classification from other systems.

Defend the network infrastructure and supporting infrastructures: This is protecting the local and wide area communications networks. It is the layer that provides confidentiality and integrity protection for data transmitted over the networks. This layer also includes implementation of supporting infrastructures such as Public Key Encryption (PKI).

Security Criteria

Leaders must ensure that a set of business rules exists that represents the enterprise's tolerance for risk. They must also enforce those security measures. Based on these risk-strategy decisions, users of the system may easily determine which behaviors are and are not acceptable.

IT/IA Acquisition

The business of information technology has become largely contractual, with businesses sending programming and data work out to areas where labor is cheap. We already have cause for concern for the insider threat, this only adds to that concern. Three years ago, the General Accounting Office, studied the use of foreign contractors by federal agencies working to fix year 2000 software problems. It found foreign nationals working on 85 contracts for "mission-critical" software. Yet several of the agencies investigated lacked even rudimentary controls over contractors' work.

As the Clinger-Cohen Act of 1996 directs that Federal Agencies ensure IT acquisitions fit into their respective IT investment portfolios, we must take additional steps to ensure that information system security becomes an integral part of the system development life cycle.

Risk Management

When reviewing information systems, we must assess the risk posed by these systems based on the following variables:

- Criticality - how important is the asset to the mission
- Vulnerability - in what ways can the asset be compromised, exploited, damaged or destroyed
- Threat - who or what can exploit vulnerability and what capabilities does that threat have that they might exploit

Once the assessment is complete, leaders may now focus risk mitigation efforts on those priority systems that are critical to operations. This process establishes a protection order of merit list from which you may apply constrained resources.

Certification and Accreditation (C&A)

Certification and accreditation is the process that validates technology devices and software as meeting the minimum requirements for information security and privacy. The purpose of a C&A is to provide a recommendation and methodology to the leadership for protecting and securing information infrastructure with a proper balance between operational mission of the system and the risk associated with those operations. The process is intended to involve the leadership in decisions about which systems are critical and how to prioritize their protection. It also provides a clear picture of risk and allows the certifier to validate what risk they are willing to accept. Figure 6 below shows the two ends of the spectrum between absolute security and the mission needs of the organization. The C&A process helps establish a clear understanding of the level of acceptable risk between the IT professionals and the organizational leadership.

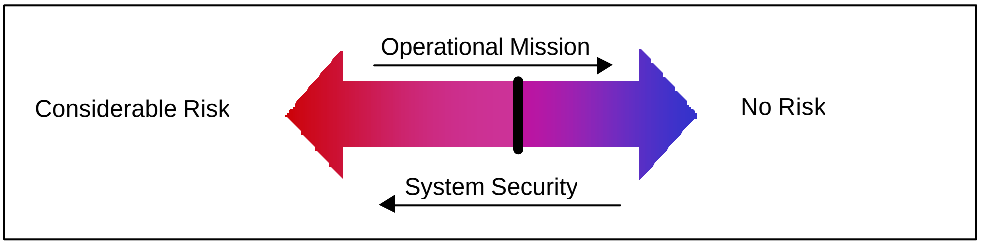

FIGURE 6 OPERATIONAL RISK VS. SYSTEMS SECURITY[22]

There are different types of accreditation depending on what is being certified:

- A system accreditation evaluates a major application or general support system.
- A site accreditation evaluates the applications and systems at a specific, self-contained location.
- A type accreditation evaluates an application or system that is distributed to a number of different locations.

Inherent to the process of accreditation is identification by the leadership, which systems are vital and which are not. The leader may then develop an implementation plan based on the perceived harm to information and potentially harmful events. The result of this detailed and exhaustive process is an operationally based implementation plan and certification document signed by the Designated Approving Authority (DAA). [23]

OPERATIONS

The operations domain of defense in depth focuses on the activities required to sustain and maintain the information security posture of the organization on a daily basis.[24] The components of the Operations domain are depicted in Figure 7.

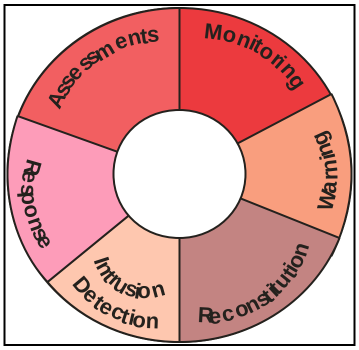

FIGURE 7 DID OPERATIONS LAYER

Assessments

Just as a good leader would defend a battle perimeter by continually assessing defensive positions, he must also continually assess network defenses. There are several methods for performing organizational assessments for information security. The method preferred by the National Security Administration (NSA) is the Information Security (INFOSEC) Methodology. [25] This assessment helps document a baseline of security. With this established baseline the enterprise may begin patching vulnerabilities in their network posture. The baseline allows for the development of metrics to determine if information security investments are working. This assessment process should begin with an audit of existing security practices before moving to the final phase of actual intrusion testing. This gives the organization an opportunity to repair existing vulnerabilities.

Monitoring

Multiple tools exist to help administrators monitor their networks. The use of system log files is generally an overlooked and often disabled function in systems administration. These logs when active tend to slow the performance of the overall system. When they are disabled however, there is seldom any mechanism to retrace the steps after an incident to determine the cause or the perpetrator. Operational policy should direct the use of system logs to ensure there is accountability and awareness within the network system.

Intrusion Detection Systems (IDS)

Unfortunately, no matter how hard you try to avoid problems with preventive measures someone may still find their way into someplace they should not be (whether it is a hacker coming in from the Internet or an employee accessing something information they should not), and therefore you must always watch for suspicious activity. Intrusion Detection devices are network and infrastructure sentries which act as motion sensors that alert security. A common error in the implementation of IDS is that they are put in place and then forgotten. They must be constantly managed to keep their software updated and the logs must be reviewed preferably on a daily basis to determine whether attempted intrusions were successful or not.

Warning

Future Neural networks will serve as warning devices for our networks. These networks are a form of multiprocessor computer system, with simple processing elements, a high degree of interconnection, simple scalar messages, and adaptive interaction between elements.[26] After base lining network behavior, network sentinels will be able to distinguish unusual network behavior and provide early warning to administrators that a network infrastructure may be under attack.

Response

We need software tools to aid in the back tracing of incidents, to discover the perpetrator. As such back tracing begins within the U.S. but then crosses country borders, we need clear laws and regulations stating which U.S. or international agencies are authorized to conduct such cyberspace pursuits, what cooperation should be expected from foreign governments and organizations, and what might be done (in real time, if possible) to disable the means by which the perpetrator is instigating the incidents.

Reconstitution

Because IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing procedures and technical measures that can enable a quick recovery of the system following a service disruption or disaster. Organizations must rehearse these plans as well write them. The first use of a contingency plan should not occur during a real disaster for this will only serve to extend the time it takes the organization to recover.

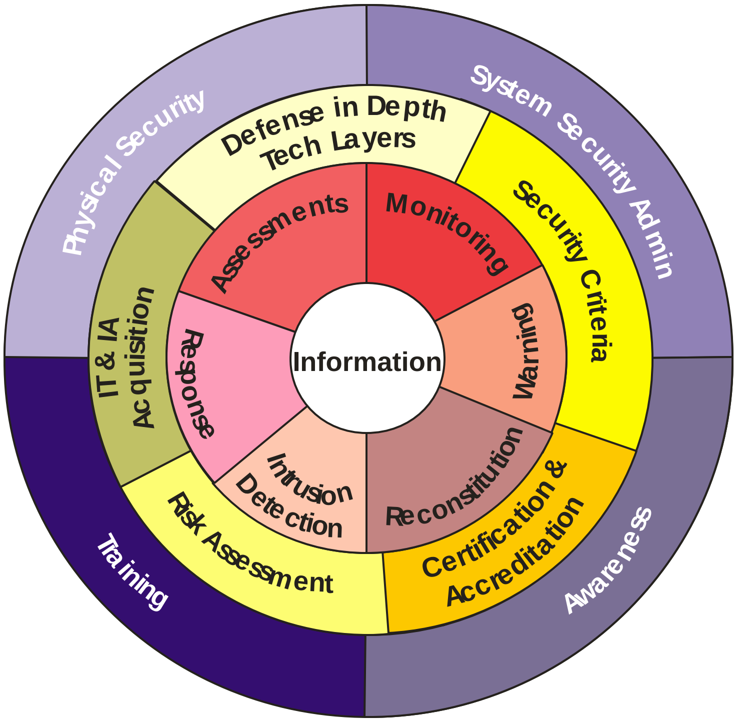

FIGURE 8 DID LAYERED DEFENSE

Finally, we arrive at our layered defense (Figure 8) that offers the attacker a potentially different picture each time they approach the system. The more doors the attacker is required to go through, the greater the risk of his/her detection. This is a best practice proven defense methodology. It provides diverse layers of defense to each attack.

COST ASSOCIATED WITH INFORMATION ASSURANCE

IT budgets for security are growing everyday yet technologists do not feel there are enough resources to accomplish the security mission. Of all the cost data collected from survey respondents in the public and private sectors, the IT security budget was one of the most significant obstacles in achieving an assured security posture.[27]

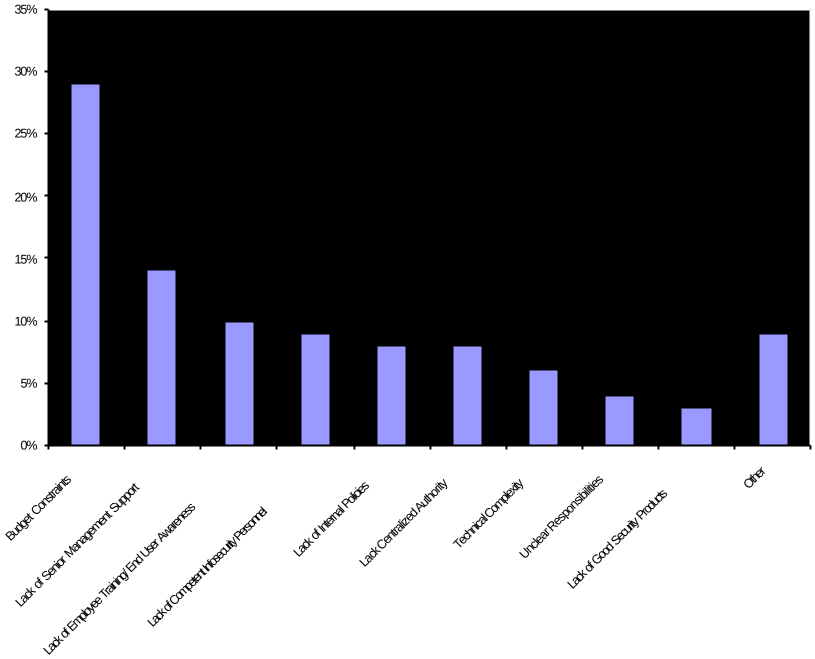

FIGURE 9 OBSTACLES TO SECURITY[28]

So how much does all of this really cost? How close are we getting to the mark and how do we determine return on investment? There are many schools of thought on how to measure the cost of information security or the cost of an attack. There is a significant cost associated with the number of cyber attacks across the globe. This cost may be represented as a loss of productivity or lost of revenue. Table 2 shows the estimated cost to industry from the most prevalent hacker attacks in recent history. As always, numbers can be misleading. These costs also include the cost to repair the systems and bring them back into service.

Name	Date	Cost in US $
Melissa	1999	1.1 Billion
Love Bug	2000	8.75 Billion
SirCam	2001	1.15 Billion
Nimda	2001	635 Million
Code Red	2001	2.62 Billion
Klez, Bugbear	2002	Unknown
Slammer	2003	Unknown

TABLE 2 ATTACK ESTIMATED COST[29]

Many organizations feel resource constraints hamper their security efforts when in fact the resource problem may be in how they actually invest their security dollars. The DOD leadership must focus resources on security knowledge and intelligence, and the effective use of intelligence. If you had only one dollar to spend on IT security, the security experts at Computer World Magazine suggest you allocate resources as depicted in Figure 10.

Cents	Category of Expense	Explanation
15	Security Policy	Spend 15 cents in nailing down the organizations overall security policy.
40	Awareness	Twenty cents to advertise the security program to general users and the other 20 cents to educate IT professionals.
10	Risk Assessment	A secure organization must understand what assets to protect, the internal and external threats and where the organization is most vulnerable.
20	Technology	Firewalls, VPNs, scanning tools, IDS, and access controls
15	Process	Security depends on management process and technology wizardry. Ongoing lifecycle development can keep networks humming for years.

FIGURE 10 HOW TO SPEND A DOLLAR ON SECURITY[30]

ALTERNATIVES TO PASSIVE DEFENSE

Alternatives to a posture of passive defense are culture paradigms we must all overcome. To counter the rapidly evolving threat capability enabled by technology, we must have a rapidly evolving leadership to meet the challenges presented by this evolving threat.

The first paradigm is an understanding that whatever we may accomplish within the Federal government defending our information systems and infrastructure will not matter if the rest of the world does not participate. Our information systems are inextricably tied to other global information systems. The adage “the chain is only as strong as its weakest link.” in today’s interconnected global information environment means “a risk accepted by one, is shared by many.” Thus only through a collaborative global effort on everyone’s part, can we achieve information assurance.

A second paradigm is that we are dealing with an incredibly rapid evolution of interconnectivity and speed. We are experiencing a technology evolution that evolves much faster than our law enforcement system’s ability to keep pace. We need legal reengineering at the global level in order to develop laws and international partnerships designed to combat cyber crime. We must not allow attackers to hide behind the very laws designed to defend this nation and our way of life.

A third paradigm is that we should treat these attacks as though they were attacks against our national interest. Allies and adversaries alike must understand that we will treat a threat to national security as a threat regardless of the manner in which it is executed.

A fourth and final paradigm is an understanding that critical infrastructure protection in the US has global implications for nation state economies as well. We must develop a clearinghouse to collect, collate, and discover patterns in cyberspace attacks that span systems in all key critical infrastructures. There are best practice models on how to cooperate on a global scale such as this. The World health Organization is an example of how global organizations work together to preclude the events from one area spreading into a global epidemic. They accomplish this through the sharing of information and subject matter expertise. They come to consensus on what actions to take to mitigate the risk as well as how to prevent a recurrence.

SUMMARY

Military commanders have long understood that information warfare is simply a fulfillment of Sun Tzu's maxim "Know your enemy and know yourself."[31] It is information dominance, which gives us the ability to gain information advantage concerning our enemy's strength and location. This information dominance exists only when the infrastructure and information systems on which it is based, are available and reliable. Our increased reliance on microchips in both military and public life makes these information systems and this nation vulnerable to an information warfare type of attack. Our increased need to interconnect these systems along with their increasing complexity exacerbates that vulnerability.

Our strategy for grappling with the increased cost of information security while facing budget decreases for information technology, force us to adopt cost saving measures that may in fact increase our vulnerability. While standardization and central management concepts like "common platform" assist in configuration and management challenges, they also make these systems more vulnerable by removing the catalyst (diversity) for survival.

Our current strategy for addressing information assurance in the acquisition process is the greatest Achilles Heel. Weapons systems are acquired and used through a life-cycle process. We do not develop the weapon and then decide that it needs ammunition. As we acquire information systems in the future, the information security aspect of the system must be included in the life cycle development process. This would ensure that security is embedded in the system thus reducing vulnerability.

We have a solid passive defense best practice strategy. We need to use it! We need a management structure that implements these security requirements and validates that the measures are in place through a series of solid metrics. We need to invest resources in the research and development of future defense systems that are more adaptive and reduce human intervention.

The information systems controlling our national infrastructure and thus our national security are some of the most complex systems ever designed. We need a better science of these complex systems, or at least tools for helping to understand their dynamic operation, complexities, and interdependencies. In order to achieve information assurance, our combined efforts must focus on active and passive defense measures, cooperation from our international partners, the evolution of law, and a change in environment that levels the playing field in this new interconnected world.

WORD COUNT=6948

ENDNOTES

[1] The National Information Systems Security (INFOSEC) Glossary, page 12, dated September 2000, Available from <http://www.nstissc.gov/Assets/pdf/4009.pdf > Internet; accessed 27 February 2004

[2] Ibid., 32.

[3] House of Representatives, Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, Information Security: *Further Efforts Needed to Fully Implement Statutory Requirements in DOD:* Available from <http://carlisle-www.army.mil/library>; Internet; accessed 21 March 2004.

[4] Information Assurance Solutions Group, "Defense in Depth, A strategy for achieving information assurance in today's highly networked environments," available from http://gd.tuwien.ac.at/pc/nsa-w2ksec/defenseindepth.pdf; Internet; accessed 15 February 2004.

[5] Hemos, Slashdot, News for Nerds, Stuff that Matters. "H1B Tech Workers Being Deported for the US." Sep 18, 2000; available from http://slashdot.org/articles/00/09/18/1652251.shtml; Internet; accessed 14 January 2004.

[6] Gartner Group. "IEEE addresses the myth of the skills shortage. Debunking the Myth of a Desperate Software Labor Shortage," available from http://www.interesting-people.org/archives/interesting-people/200310/msg00156.html; Internet; accessed 16 February 2004.

[7] Gartner Group EXP Club, "Information Security— How Much Is Enough?" available from http://www.gartner.com/EXP/114348.pdf; Internet; accessed 18 Dec 2003.

[8] Ibid.

[9] JANE'S Special Report on "TERRORISM & SECURITY MONITOR", (1 August 2001): [database on-line]; available from Janes; accessed 12 January 2004.

[10] Ibid.

[11] Government Computer News, "Don't Worry, Be Hacked" available from <http://Safe@HomeInformationAssurancein the Homeland Security Era - Page 3.htm >; Internet; accessed 18 December 2003.

[12] Computer Emergency Response Team (CERT), Carnegie Mellon University's Software Engineering Institute; available from http://www.cert.org; Internet; accessed 19 January 2004.

[13] Ibid., House of Representatives.

[14] Ibid., Computer Emergency Response Team.

[15] *10th United States Code*, Planning and Coordination, Chapter13, (May 2000).

[16] William A. Wulf, Ph.D. President, National Academy of Engineering before the House Science Committee U.S. House of Representatives October 10, 2001.

[17] National Security Agency, *Defense-in-Depth, Information Assurance Technical Framework* Release 3.1September 2002.

[18] Ibid., Information Assurance Solutions Group

[19] Ibid.

[20] Garner Group, *Technology Hype Cycle for Network Defense* , available from http://www4.gartner.com/hc/asset_50595.jsp; Internet; accessed 18 Dec 2003.

[21] Ibid.

[22] Gil Duvall, "Certification and Accreditation," lecture, Fort McNair, National Defense University, Information Resources Management College, February 2004, cited with permission of Professor Gil Duvall.

[23] The Designated Approval Authority is the Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk.

[24] Ibid., Information Assurance Solutions Group.

[25] National Security Agency, "INFOSEC Methodology," available from http://www.nsa.gov/isso/iam/index.htm Internet; Accessed on 3 March 2004.

[26] Leslie Smith, "An Introduction to Neural Networks," Center for Cognitive and Computational Neuroscience, Department of Computing and Mathematics. University of Sterling, 25 October 1996 Available from http://www.cs.stir.ac.uk/~lss/NNIntro/InvSlides.html#what; Internet; accessed 6 April 2004.

[27] Information Security Magazine, Enough Is (Never) Enough, July 1999, Available from www.Infosecuritymag.com/articles/1999/enough.shtml; Internet; accessed 4 March 2004.

[28] Ibid.

[29] Ibid., Information Security 32

[30] Ibid., Gil Duvall

[31] Tzu, Sun. *The Art of War*, trans. Samuel B. Griffith (Oxford Press, June 1971).

GLOSSARY

Abuse of Privilege	When a user performs an action that they should not have, according to organizational policy or law.
Access	The ability to enter a secured area. The process of interacting with a system. Used as either a verb or a noun.
Access Authorization	Permission granted to users, programs or workstations.
Access Control	A set of procedures performed by hardware, software and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.
Access Sharing	Permitting two or more users simultaneous access to file servers or devices.
Alphanumeric Key	A sequence of letters, numbers, symbols and blank spaces from one to 80 characters long.
ANSI	The American National Standards Institute. Develops standards for transmission storage, languages and protocols. Represents the United States in the ISO (International Standards Organization).
Application-Level Firewall	A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.
Audit	The independent examination of records to access their veracity and completeness.
Audit Trail	An audit trail may be on paper or on disk. In computer security systems, a chronological record of when users log in, how long they are engaged in various activities, what they were doing, whether any actual or attempted security violations occurred
Authenticate	In networking, to establish the validity of a user or an object (i.e. communications server).
Authentication	The process of establishing the legitimacy of a user (or node) before allowing access to requested information. An example is for the user to enter a name or account number (identification) and password (authentication).
Authentication Tool	A software or hand-held hardware "key" or "token" utilized during the user authentication process. See key and token.
Authentication Token	A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords.
Authorization	The processes of determining what types of activities are permitted. Usually, authorization is in the context of authentication. Once you have authenticated a user, the user may be authorized different type of access or activity.
Availability	Ensuring that authorized users have access to information and associated assets when required.

Back Door	An entry point to a program or a system that is hidden or disguised often created by the software's author for maintenance. A certain sequence of control characters permits access to the system manager account. If the back door becomes known, unauthorized users (or malicious software) can gain entry and cause damage.
Bastion Host	A system that has been hardened to resist attack, and which is installed on a network in such a way that it is expected to come under attack. Bastion hosts are often components of firewalls, or may be "outside" Web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (e.g., UNIX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system.
Biometric Access Control	Any means of controlling access through human measurements, such as fingerprinting and voice printing.
CA (Certificate Authority)	A CA is an authority that issues and manages security credentials for a PKI.
CA Private Root Key	A cryptographic key known only to the CA is used to certify user or server certificate requests (Digitally sign certificate)
CERT	The Computer Emergency Response Team was established at Carnegie-Mellon University after the 1988 Internet worm attack.
Challenge/Response	A security procedure in which one communicator requests authentication of another communicator, and the latter replies with a pre-established appropriate reply.
Chroot	A technique under UNIX whereby a process is permanently restricted to an isolated subset of the file system.
Cipher	Alternative term for an encryption algorithm.
Ciphertext	Text (or data) that has previously been encrypted.
Coded File	In encryption, a coded file contains unreadable information.
Communications Security	Procedures designed to ensure that telecommunications messages maintain their integrity and are not accessible by unauthorized individuals.
Computer Security	Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.
Computer Security Audit	An independent evaluation of the controls employed to ensure appropriate protection of an organization’s information assets.
Confidentiality	Ensuring that information is accessible only to those authorized to have access.
Cryptographic Checksum	A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference. Checksum systems are a primary means of detecting file system tampering on UNIX.
Data Driven Attack	A form of attack in which a user or other software to implement an attack encodes the attack in innocuous-seeming data that is executed. In the case of firewalls, a data driven attack is a concern since it may get through the firewall in data form and launch an attack against a system behind the firewall.
Data Encryption Standard	An encryption standard developed by IBM and then tested and adopted by the National Bureau of Standards. Published in 1977, the DES standard has proven itself over nearly 20 years of use in

	both government and private sectors.
Data Encryption Key	DEK - Used for the encryption of message text and for the computation of message integrity checks (signatures).
DEK	Used for the encryption of message text and for the computation of message integrity checks (signatures).
Encryption	The way to make data unreadable to everyone except the recipient of the data. Encryption is often used to make the transmission of credit card numbers secure for those who are shopping using the Internet. Secure sites use encryption.
Decode	Conversion of encoded text to plaintext through the use of a code.
Decrypt	Conversion of either encoded or enciphered text into plaintext.
Dedicated	A special purpose device. Although it is capable of performing other duties, it is assigned to only one.
Defense in Depth	The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.
DES	Data encryption standard.
Digital Certificate	A digital identifier linking an entity and a trusted third party with the ability to confirm the entity's identification. Typically stored in a browser or a smart card.
DNS Spoofing	Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.
Dual Homed Gateway	A dual homed gateway is a system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a dual homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks.
Encrypting Router	See Tunneling Router and Virtual Network Perimeter.
Encryption	The process of scrambling files or programs, changing one character string to another through an algorithm (such as the DES algorithm).
End-to-End Encryption	Encryption at the point of origin in a network, followed by decryption at the destination.
Environment	The aggregate of external circumstances, conditions and events that affect the development, operation and maintenance of a system.
Firewall	A system or combination of systems that enforces a boundary between two or more networks. This will prevent unauthorized personnel from interfering with a computer or network.
Gateway	A bridge between two networks.
Global Security	The ability of an access control package to permit protection across a variety of mainframe environments, providing users with a common security interface to all.
Granularity	The relative fineness or coarseness by which a mechanism can be adjusted.

Hack	Any software in which a significant portion of the code was originally another program.
Host-based Security	The technique of securing an individual system from attack. Host-based security is operating system and version dependent.
Hot Standby	A backup system configured in such a way that it may be used if the system goes down.
IETF	The Internet Engineering Task Force, a public forum that develops standards and resolves operational issues for the Internet. IETF is purely voluntary.
Information Security	Preservation of confidentiality, integrity and availability of information.
Information	All media (printed or written on paper, stored electronically, transmitted by post or fax, shown on films, or spoken in conversation). BS7799 standard also recognizes new methods of doing business, such as e-commerce, the internet, outsourcing and all other forms of information and data, including voice, graphics and media such as mobile phones.
Information Systems Technology	The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.
Insider Attack	An attack originating from inside a protected network.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Internet (Today)	A web of different, intercommunicating networks funded by both commercial and government organizations. It connects networks in 40 countries. No one owns or runs the Internet. There are thousands of enterprise networks connected to the Internet, and there are millions of users, with thousands more joining every day.
Intrusion Detection	Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.
IP Splicing/Hijacking	An attack whereby an active, established, session is intercepted and co-opted by the attacker. IP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer.
IP Spoofing	An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.
ISO	International Organization for Standardization sets standards for all types of topics including data communications.
ISO17799: 2000	Code of Practice for Information Security Management. A standard that provides guidance on the management of information security.
ISSA	International Systems Security Association.

Key	In encryption, a key is a sequence of characters used to encode and decode a file. You can enter a key in two formats: alphanumeric and condensed (hexadecimal). In the network access security market, "key" often refers to the "token," or authentication tool, a device utilized to send and receive challenges and responses during the user authentication process. Keys may be small, hand-held hardware devices similar to pocket calculators or credit cards, or they may be loaded onto a PC as copy-protected, software.
Least Privilege	Designing operational aspects of a system to operate with a minimum amount of system privilege. This reduces the authorization level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorized activity resulting in a security breach.
Local Area Network (LAN)	An interconnected system of computers and peripherals. LAN users share data stored on hard disks and can share printers connected to the network.
Logging	The process of storing information about events that occurred on the firewall or network.
Log Processing	How audit logs are processed, searched for key events, or summarized.
Log Retention	How long audit logs are retained and maintained.
Network-Level Firewall	A firewall in which traffic is examined at the network protocol packet level.
Network Worm	A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability or availability. A network worm may attack from one system to another by establishing a network connection. It is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network.
One-Time Password	In network security, a password issued only once as a result of a challenge-response authentication process. Cannot be "stolen" or reused for unauthorized access.
Operating System	The layer of software that sits between a computer and an application, such as an accounting system or E-mail.
Orange Book	The Department of Defense Trusted Computer System Evaluation Criteria. It provides information to classify computer systems, defining the degree of trust that may be placed in them.
Password	A secret code assigned to a user. Also known by the computer system. Knowledge of the password associated with the user ID is considered proof of authorization. (See One-Time Password.)
Perimeter-based Security	The techniques of securing a network by controlling access to all entry and exit points of the network.
PIN	In computer security, a personal identification number used during the authentication process. Known only to the user. (See Challenge/Response, Two-Factor Authentication.)
Policy	Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Private Key	In encryption, one key (or password) is used to both lock and unlock data. Compare with public key.
Protocols	Agreed-upon methods of communications used by computers.
Proxy	A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.
Public Key	In encryption, a two-key system in which the key used to lock data is made public, so everyone can "lock." A second private key is used to unlock or decrypt.
Risk Analysis	The analysis of an organization’s information resources, existing controls and computer system vulnerabilities. It establishes a potential level of damage in dollars and/or other assets.
Risk management	Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost
Risk Assessment	Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence
Rogue Program	Any program intended to damage programs or data. Encompasses malicious Trojan Horses.
RSA	A public key cryptosystem named by its inventors, Rivest, Shamir and Adelman, who hold the patent.
Session Stealing	See IP Splicing.
Smart Card	A credit-card-sized device with embedded microelectronic circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.
Social Engineering	An attack based on deceiving users or administrators at the target site. Telephoning users or operators and pretending to be an authorized user, to attempt to gain illicit access to systems, typically carry out social engineering attacks.
Screened Host	A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router.
Screened Subnet	A subnet behind a screening router. The degree to which the subnet may be accessed depends on the screening rules in the router.
Screening Router	A router configured to permit or deny traffic based on a set of permission rules installed by the administrator.
Secure Socket Layer	A method of encrypting data as it is transferred between a browser and Internet server. Important for online payments.
Signature	A personal tag automatically appended to an email message. May be short, such as the author's name, or quite long, such as a favorite quote.
SSL	Secure Socket Layer - A method of encrypting data as it is transferred between a browser and Internet server. Important for online payments.

Statement Of Applicability	Summary and justification of implemented and non-implemented information security objectives and controls applicable to the needs of the organization
Token	A "token" is an authentication too, a device utilized to send and receive challenges and responses during the user authentication process. Tokens may be small, hand-held hardware devices similar to pocket calculators or credit cards. See key.
Trojan Horse	A computer program which carries within itself a means to allow the creator of the program access to the system using it.
Tunneling Router	A router or system capable of routing traffic by encrypting it and encapsulating it for transmission across an un-trusted network, for eventual de-encapsulation and decryption.
Two-Factor Authentication	Two-factor authentication is based on something a user knows (factor one) plus something the user has (factor two). In order to access a network, the user must have both "factors" - just as he/she must have an ATM card and a Personal Identification Number (PIN) to retrieve money from a bank account. In order to be authenticated during the challenge/response process, users must have this specific (private) information.
User	Any person who interacts directly with a computer system.
User ID	A unique character string that identifies users.
User Identification	User identification is the process by which a user identifies himself to the system as a valid user. (As opposed to authentication, which is the process of establishing that the user is indeed that user and has a right to use the system?)
Virtual Network Perimeter	A network that appears to be a single protected network behind firewalls, which actually encompasses encrypted virtual links over un-trusted networks.
Virus	A program, which replicates itself on computer systems by incorporating itself into other programs, which are shared among computer systems. Viruses may or may not contain attack programs or trapdoors.
Worm	A computer program, which replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments.

Source: The National Information Systems Security (INFOSEC) Glossary

BIBLIOGRAPHY

Adams, James. *The Next World War, Computers are the Weapons & the Front Line is Everywhere.* Simon & Schuster, 1998

Berkowitz, Bruce, *The New Face of War: Chapter 13, 'An Electronic Pearl Harbor*?", pp 135-154 available from < http://www.ndu.edu/icaf/departments/ltis/l5.htm >; Internet; accessed 23 Jan 2004

Bush, George W. *Critical Infrastructure Protection in the Information Age.* Presidential Executive Order 13231, Washington D.C.: The White House, October 2001.

Bush, George W. *National Strategy to Secure Cyberspace.* Washington D.C.: The White House, February 2003.

Clinger-Cohen Act. Role of the CIO (1996).

Cohen, Fred & Associates. "Strategic Security & Intelligence," available from <http://all.net>; Internet ; accessed 4 March 2004.

Computer Emergency Response Team (CERT), Carnegie Mellon University's Software Engineering Institute. Available from HTTP://WWW.CERT.ORG Internet, Accessed on 19 January 2004

Farrell, Peter T. *A National Security Strategy for Information Assurance Authors.* Army War College Strategic Studies Institute; U.S. Army War College,

Federal Information Security Management Act. Information Security (2002).

Gartner Group EXP Club Reports, "Information Security-How Much is Enough?" April 2003

Gartner Group, "IEEE addresses the myth of the skills shortage. Debunking the Myth of a Desperate Software Labor Shortage." available from <http://www.interesting-people.org/archives/interesting-people/200310/msg00156.html>; Internet; accessed 16 February 2004.

Government Computer News, "..Don't Worry, Be Hacked" Thursday January 8, 2004 | Updated 7:25 PM EST January 7, Available from <HTTP://Safe @ Home Information Assurance in the Homeland Security Era - Page 3.htm> Internet; accessed 18 December 2003

Hemos, Slashdot, News For Nerds, Stuff that Matters. H1B Tech Workers Being Deported for the US. Posted on Mon Sep 18, '00 09:52 PM Available from <http://slashdot.org/articles/00/09/18/1652251.shtml>; Internet; Accessed on 14 January 2004

Herb Lin, *Cyber-security Today and Tomorrow*: *Pay Now or Pay Later*. Washington, D.C. National Academy Press., 2002. Available from <http://www.cstb.org>; Internet; accessed 23 February.

Information Security Magazine July 1999 Available from <http;//www.Infosecuritymag.com/articles/1999/enough.shtml>; Internet; accessed 4 March 2004

JANE'S Special Report on “TERRORISM & SECURITY MONITOR”, (1 August 2001): Database on-line. Available from Janes. Accessed 12 January 2004.

Mitnick, Kevin, and Simon, William. *The Art of Deception, Controlling the Human Element of Security.* Indianapolis: Wiley Publishing Inc., 2002.

National Security Agency, *Defense in Depth, A Strategy for achieving Information Assurance in today’s highly networked environments,* available from http://gd.tuwien.ac.at/pc/nsa-w2ksec/defenseindepth.pdf; Internet; accessed 15 February 2004.

National Security Telecommunications and Information Systems Policy (NSTISSP), *National IA Acquisition Policy,* National Security Directive (NSD) No. 42, July 1990.

National Security Telecommunications and Information Systems Security Committee. *National Information Assurance Acquisition Policy No. 11*, January 2000, available from <http://www.nstissc.gov/Assets/pdf/nstissp11.pdf>; Internet, accessed 12 February 2004

SANS Institute and the Federal Bureau of Investigation. “The Twenty Most Critical Internet Security Vulnerabilities—The Experts’ Consensus.” available from http://www.sans.org/top20; Internet; accessed 18 February 2004.

The Information Assurance Advisory Council, “A National R&D Strategy for Information Assurance.” Available from http://www.iaac.org.uk/Publications/flyers/ R_and_Dv3.pdf; Internet. Accessed 18 December 2003.

The National Information Assurance Partnership (between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) website. Available from http://niap.nist.gov; Internet. Accessed 18 December 2003.

The National Information Systems Security (INFOSEC). “Glossary” Available from http://www.nstissc.gov/Assets/pdf/4009.pdf; Internet; accessed 14 February 2004.

U.S. Department of Defense, *Discretionary Guidebook,* Department of Defense Instruction Regulation 5000.2-R. Washington, D.C.: U.S. Department of Defense, 12 May 2003.

U.S. Department of Defense, *Information Assurance Implementation,* Department of Defense Instruction 8500.2. Washington, D.C.: U.S. Department of Defense, 24 October 2002.

U.S. Department of Defense, *Information Assurance,* Department of Defense Directive 8500.1. Washington, D.C.: U.S. Department of Defense, 24 October 2002.

U.S. Department of Defense, Operation *of the Defense Acquisition System,* Department of Defense Instruction 5000.2. Washington, D.C.: U.S. Department of Defense, 12 May 2003.

U.S. Department of Defense, the *Defense Acquisition System* . Department of Defense Directive 5000.1. Washington, D.C.: U.S. Department of Defense, 12 May 2003.

Verton, Dan. *Black Ice, The invisible Threat of Cyber-Terrorism* , McGraw-Hill, 2003

Wulf, William A. Ph.D. President, National Academy of Engineering before the House Science Committee U.S. House of Representatives October 10, 2001.